Un estudio comparativo en extensiones de seguridad para el sistema de nombres de dominio. Resultados finales

Sánchez Ernesto, Arias Figueroa Daniel, Rocabado Sergio, Agüero Verónica, Molina Gustavo.

C.I.D.I.A./Departamento de Informática/Facultad de Ciencias Exactas/Universidad Nacional de Salta
Av. Bolivia 5150. 0387-4255547

esanchez@cidia.unsa.edu.ar; daaf@cidia.unsa.edu.ar; srocabad@cidia.unsa.edu.ar; Vero_m13@hotmail.com; gustavo_molina323@hotmail.com

Resumen

Para cubrir los aspectos de seguridad del protocolo DNS, DNSCurve se presenta como una alternativa, que mediante criptografía de clave pública/privada, permite encriptar y autenticar los paquetes de datos intercambiados entre Servidores Resolvers y Servidores Autoritativos. El protocolo fue diseñado por Daniel J. Bernstein y está basado en el uso de criptografía de curva elíptica, más precisamente, Curve25519. El presente trabajo presenta resultados sobre la evaluación de esta alternativa, en el marco del proyecto de investigación Nº 1223/0: "Extensiones de Seguridad para el Sistema de Nombres de Dominio", del Consejo de Investigación de la UNSa. Se expondrán los aspectos relacionados a la implementación de DNSCurve, y evaluación de comportamiento mediante la simulación de tráfico, lo que permitió obtener datos estadísticos basados en consultas DNS, análisis de los mismos y conclusiones sobre el rendimiento obtenido en un servidor con estas características.

Palabras clave:

Internet, Sistema de Nombres de Dominio, DNSCurve, Criptografía de curva elíptica.

Contexto

El presente trabajo expone los resultados obtenidos en el marco del proyecto de investigación "Extensiones de Seguridad para el Sistema de Nombres de Dominio" (Consejo de Investigación de la Universidad Nacional de Salta), en conjunto con el Centro de Investigación y Desarrollo en Informática Aplicada (C.I.D.I.A. – UNSa).

Introducción

En referencia a aspectos de seguridad para el Sistema de Nombres de Dominio, son dos las alternativas que han sido motivo de investigación, con el propósito de alcanzar una implementación a escala global. Estas son; Extensiones de Seguridad para DNS (DNSSEC) y DNSCurve. Con respecto a la primera, tales extensiones, proveen autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS. Las mejoras que ofrece DNSSEC radican principalmente en el uso de una

jerarquía de "firmas criptográficas" que permite proteger el flujo de información intercambiado entre Servidores Autoritativos, Servidores DNS Recursivos y Clientes DNS. [1]. En base a lo expuesto anteriormente, y según se describe en el RFC 4033, se observa una de las limitaciones presentes en el diseño de estas extensiones de seguridad, la misma radica en la ausencia de confidencialidad del flujo de datos intercambiados en el proceso de resolución de nombres, ya que una respuesta DNSSEC es autenticada pero no encriptada. Así también, y en base a las investigaciones realizadas, se puede considerar como una limitación, que para garantizar la autenticación e integridad, es necesario la construcción de una "cadena de confianza", proceso mediante el cual cada nodo involucrado en el proceso de resolución, debe "confiar" en el nodo inmediatamente superior, hasta llegar a los nodos raíz.

Por otro lado, la alternativa DNSCurve [2] se presenta como un nuevo protocolo de seguridad para DNS, que utiliza la estructura jerárquica del mismo, para propagar la confianza mediante la incorporación de claves públicas, permitiendo encriptar y autenticar los paquetes de datos intercambiados entre Resolvers y Servidores Autoritativos [3]. El protocolo fue diseñado por Daniel J. Bernstein y está basado en el uso de criptografía de curva elíptica, más precisamente, Curve25519.

El propósito de DNSCurve es cubrir los siguientes aspectos de seguridad:

- Confidencialidad, mediante la encriptación de todas las consultas y sus correspondientes respuestas, en un proceso de resolución de nombres.
- Integridad, mediante la encriptación criptográfica de todas las respuestas DNS.
- Disponibilidad, mediante una rápida detección y posterior eliminación de paquetes DNS falsos.

Tomando como base estas dos alternativas, desde el Centro de Investigación y Desarrollo en Informática Aplicada (C.I.D.I.A.) y en el marco del proyecto de investigación Nº 1223/0: "Extensiones de Seguridad para el Sistema de Nombres de Dominio" del Consejo de Investigación de la Universidad Nacional de Salta, se desarrollaron tareas de estudio del estado del arte tanto de DNSSEC como de DNSCurve, implementación de ambientes de pruebas que permitan realizar estimaciones de consumos de recursos tales como ancho de banda, uso de memoria y procesador y aspectos relacionados a la integración de ambas, con la finalidad de obtener una arquitectura DNS segura.

El presente trabajo está centrado en mostrar los aspectos relacionados a la implementación de DNSCurve, y evaluación de comportamiento mediante la utilización de un prototipo de software desarrollado para la simulación de tráfico, lo que permitió obtener datos estadísticos basados en consultas DNS, análisis y conclusiones sobre el rendimiento obtenido en un servidor con estas características.

Líneas de Investigación, Desarrollo e Innovación

Los principales ejes temáticos que se están investigando son los siguientes:

- Sistema de Nombres de Dominio.
- Criptografía de clave pública.
- DNSCurve.

.

Resultados y Objetivos

Durante las etapas de investigación se montaron diferentes escenarios de pruebas, con errores de funcionamiento en los primeros casos, debido a la escasa documentación de instalación y configuración encontrada al respecto. Finalmente se seleccionan dos escenarios, siendo el primero el ambiente donde se realizó el seguimiento de un proceso de consulta/respuesta y análisis de paquetes de datos. El segundo escenario permitió realizar un análisis de rendimiento (consultas procesadas y longitud de paquetes DNSCurve) comparando un servidor DNS estándar frente a un servidor DNSCurve.

A continuación se describen ambos escenarios junto a los resultados obtenidos.

Escenario de prueba para análisis de traza DNSCurve.

Con el escenario de prueba montado se procedió a realizar el seguimiento de una consulta enviada desde el cliente DNS hacia el Servidor DNSCurve, para el dominio dnscurve.org. Para la captura y análisis de tráfico se utilizó la herramienta Wireshark [6].

El seguimiento de la traza permitió observar que; en un servidor DNS Resolver con característica DNSCurve, todo el tráfico saliente, así como el tráfico entrante, es automáticamente encriptado haciendo uso de criptografía de curva elíptica (Curve 25519). Cuando el Resolver, contacta a un Servidor Autoritativo, comprueba si este contiene una clave pública DNSCurve con el formato correcto. Si la clave secreta por parte del Resolver es c, entonces la correspondiente clave pública es Curve25519(c), del mismo modo ocurre para el servidor autoritativo, considerando que su clave privada es s, la correspondiente clave pública es Curve25519(s). Las claves se componen de la cadena de caracteres “uz5”, seguido de una cadena de 51 bytes codificados con la clave pública del servidor. Las claves públicas para un servidor autoritativo, se transportan sobre registros NS, de esta manera, un Resolver sabe que el servidor consultado soporta DNSCurve. De esta manera, el Resolver, puede de manera simple, encriptar y autenticar los paquetes que este envía al Autoritativo. Por su parte, el Resolver envía al servidor consultado, un paquete expandido que contiene su clave pública DNSCurve, un número (nonce), de 96 bits de longitud y una “cryptobox” que contiene el mensaje original, el cual es básicamente la consulta realizada. Para la creación de la “cryptobox”, el Resolver usa su clave privada, el nonce del paquete y su clave pública. El servidor que recepciona la consulta, abre esta caja, utilizando su clave privada, más la clave pública del Resolver y el nonce del paquete. Como respuesta, el servidor consultado, envía un paquete expandido que contiene un nonce (de 96 bits) diferente al recibido, más su “cryptobox”. De igual manera que lo hizo el Servidor Autoritativo, el Resolver, utiliza su clave secreta DNSCurve, la clave pública del Autoritativo y el nonce, para desencriptar la “caja” recibida. Si la apertura de esta caja fallara, podría significar que el mensaje ha sido falsificado, por lo tanto, el Resolver, simplemente descarta el paquete y queda a la espera de una respuesta legítima.

Otro aspecto importante en el seguimiento de la traza es que al viajar la consulta y su correspondiente respuesta encriptadas, Wireshark no puede acceder a los contenidos, mostrando al paquete DNS como malformado.

Escenario de prueba para análisis de rendimiento servidor DNSCurve.

El análisis de rendimiento se realizó en base a las consultas procesadas, se crearon cinco configuraciones diferentes de prueba. Cada configuración se distingue de la otra por la cantidad de consultas por segundo. La cantidad de consultas por segundo que se usaron para este estudio comparativo son 250, 500, 750, 1000 y 1250.

La primera observación que puede realizarse en base a los resultados obtenidos, es que el servidor DNS estándar alcanza a procesar el 95% de las consultas recibidas, mientras que a un servidor CurveDNS alcanza un 39%, con una baja en el rendimiento superior al 50% a medida aumenta la cantidad de consultas por segundo. Al analizar las causas de la caída en el rendimiento, se pudo observar que al recibir las consultas y no disponer de sockets para el reenvío de las mismas, tales consultas se descartan.

Al aumentar la cantidad de consultas enviadas por segundo (4000qps), se puede presentar una generalización del comportamiento del servidor CurveDNS, de manera tal que a medida que las consultas recibidas se incrementan de manera logarítmica, la cantidad de consultas perdidas se incrementan de manera exponencial.

Comparativa longitud de consulta DNS estándar frente a consulta DNSCurve.

Con el propósito de realizar estimaciones de consumo de ancho de banda, se analizaron longitud de un paquete DNS estándar frente a un paquete DNSCurve. Para tales pruebas se hizo uso de un generador de consultas desarrollado en lenguaje Python, y un conjunto de librerías [4], que permitieron la creación de las claves públicas y privadas, así como la cryptobox Para el desarrollo del generador, se tomó como base el prototipo creado por Harm H. A. Van Tilborg [5].

El desarrollo se divide en dos partes: “dnsQueryGenerator” y “dnsQuerySender”. La primera, genera un archivo que contiene las consultas; para ello se necesita un archivo de configuración, que contiene los parámetros necesarios para generar las consultas, esto es, minutos de ejecución, cantidad de consultas por segundo, porcentaje de consultas DNSCurve, porcentaje de consultas erróneas para un determinado tipo de registro de recurso, entre otros; y otro archivo que contenga un listado de dominios. La segunda parte recibe como entrada este archivo de consultas generado, lee las mismas y las envía.

Mediante la ejecución de un script que realiza la lectura de un determinado archivo de consultas generado por el “dnsQueryGenerator”, se calcularon las longitudes de cada consulta presentes en este archivo, posteriormente se calculó el promedio del tamaño de las consultas, luego de generar 75000 consultas.

Como resultado, se observó que el tamaño de un paquete DNS estándar en

proporción es aproximadamente un tercio en relación a un paquete DNSCurve, lo que introduce un retardo en la transmisión del paquete; que no afecta de manera significativa el rendimiento, por lo que se podría no tener en cuenta.

En conclusión, la alternativa DNSCurve es producto de la investigación y desarrollo personal, a diferencia de la alternativa DNSSEC, que actualmente se encuentra impulsada a escala global por organizaciones como la ICANN, Verisign, IANA, entre otros

En términos generales, DNSCurve aún no ha sido adoptada por la comunidad de Internet como una alternativa a implementar a escala global, a diferencia de la alternativa DNSSEC, que desde el año 2010 ya la implementan los servidores raíces [7], y son cada vez más los dominios de nivel superior que la han incorporado [8]. Sin embargo, consideramos que DNSCurve debe ser incorporado como parte de un conjunto de soluciones, con el propósito de abarcar todos los aspectos de seguridad en el Sistema de Nombres de Dominio.

Formación de Recursos Humanos

La estructura del equipo de investigación es de 5 (cinco) miembros incluidos el Director y Co-director.

Dos miembros aprobaron trabajo de Tesis de Posgrado en Redes de Datos, dependiente de la Universidad Nacional de La Plata.

Otros dos participantes aprobaron trabajo de Tesis de Grado (DNS Curve), de la Carrera de Licenciatura en Análisis de Sistemas de la Universidad Nacional de Salta.

Referencias

[1] ARENDS, R., AUSTEIN, R., LARSON, M., MASSEY, D., AND ROSE, S. RFC 4033: DNS Security Introduction and Requirements, Marzo 2005.

[2] DNSCurve: Usable security for DNS. http://dnscurve.org. Fecha de consulta: Setiembre 2014.

[3] Sabbir Ahmmed. DNS Privacy & Confidential DNS. Seminar Report: Network & Communications Privacy. Alemania. Mayo 2014.

[4] NaCl: Networking and Cryptography library. Computer Aided Cryptography Engineering. http://nacl.cace-project.eu/. Fecha de consulta: Diciembre 2014.

[5] Harm H. A. Van Tilborg. Shaping DNS security with curves. Technische Universiteit Eindhoven, Países Bajos. 2010.

[6] WIRESHARK. GNU GENERAL PUBLIC LICENSE Version 2, June 1991 .Copyright (C) 1989, 1991 Free Software Foundation,

[7] Root DNSSEC. Information about DNSSEC for the Root Zone. http://www.root-dnssec.org/. Fecha de consulta: Dic. 2014.

[8] Internet Society. DNSSEC Statistics. http://www.internetsociety.org/deploy360/dnssec/statistics/. Fecha de consulta: Dic. 2014.